What is claimed is:

1. A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by:
   (a) modifying the message data with additional data, and
   (b) then encrypting said modified message data using a private key of a public-private key pair stored within the computer chip.

2. A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by:
   (a) modifying the message data by appending additional data thereto,
   (b) calculating a hash value of said modified message data, and
   (c) then encrypting said calculated hash value using a private key of a public-private key pair.

3. The method of claim 2, wherein said step of modifying comprises appending the additional data to the message data.

4. The method of claim 2, wherein said step of modifying comprises embedding the additional data within the message data.

5. The method of claim 2, wherein the additional data comprises data prestored within memory of the computer chip.

6. The method of claim 2, wherein the additional data represents a verification status of the device.

7. The method of claim 2, wherein the message data includes a field identifier corresponding to a field of data prestored within the memory of the computer chip, the field identifier having a null value, and wherein said step of modifying the message data comprises retrieving the value stored in the memory location identified by the field identifier and embedding said retrieved value in the message data with the field identifier.

8. The method of claim 7, wherein the memory of the computer chip in which the additional data is stored is content searchable memory.

9. The method of claim 7, wherein the message data comprises XML formatting.

10. A method for extracting user information from a computer chip, the computer chip including content searchable memory in which different fields of data are prestored, comprising transmitting an identifier of a particular field of data prestored within the computer chip together with a null value therefor.

11. The method of claim 10, wherein the identifier and null value therefor transmitted to the computer chip comprise XML formatting.

12. A method of obtaining a random number for utilization in an application requiring a random number, comprising generating a digital signature using a digital signature algorithm, and then using said generated digital signature as the random number in the application.

13. The method of claim 12, further comprising the step of using the digital signature as a random number to safeguard against a replay attack.

14. The method of claim 12, further comprising the step of using the digital signature to generate a session key for secure electronic communications.

15. The method of claim 12, wherein the digital signature is generated within a computer chip.

16. The method of claim 15, wherein the computer chip includes a random number generator.

17. The method of claim 16, wherein the digital signature is generated within the computer chip using a private key of a public-private key pair and a random number obtained from the random number generator.

18. The method of claim 17, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

19. The method of claim 18, wherein the random number generator is directly inaccessible from outside of the computer chip.

20. The method of claim 18, wherein the random number generator is accessible only by a digital signature circuit.